



DEPARTMENT OF THE NAVY

COMMANDER
NAVY REGION, MID-ATLANTIC
1510 GILBERT ST.
NORFOLK, VA 23511-2737

IN REPLY REFER TO:

COMNAVREGMIDLANT
INST 2305.1
N112

12 JAN 2004

COMMANDER, NAVY REGION, MID-ATLANTIC INSTRUCTION 2305.1

Subj: POLICIES AND PROCEDURES GOVERNING THE USE OF THE SECURE TELEPHONE
UNIT VERSION III (STU-III) TYPE 1 TERMINAL

Ref: (a) Director, COMSEC Material System manual CMS-21A
(b) Secure Telephone Unit Third Generation (STU-III) COMSEC
Material Management Manual (CMS-6)
(c) STU-III Key Management Plan EKMS-702.01
(d) NTISSI No. 3013 of 8 Feb 90

Encl: (1) STU-III COMSEC Material Responsible Acknowledgement

1. Purpose. To publish policy, guidance and instructions concerning the use and security of the STU-III secure telephone.

2. Cancellation. COMNAVBASENORVASTAFFINST 2305.1

3. Background. The STU-III was designed as a modern desktop device capable of operating in the secure voice and data mode in an administrative office. The STU-III terminal is designed to protect sensitive/classified information at all levels up to Top Secret Sensitive Compartmented Information (SCI). STU-III's are secure voice terminals and are to be installed and maintained by the STU-III custodian or appointed Local Element custodians.

a. All STU-III COMSEC material must be stored and protected per chapter 5 of reference (a), for the level of classification of the material.

b. STU-III Communication Security (COMSEC) material is distributed through the Electronic Keying Material System (EKMS) manager to registered STU-III COMSEC Accounts (SCA).

(1) The Director, COMSEC Material System (DCMS) provides accountability controls for STU-III terminals. These controls are published in reference (b).

(2) The EKMS Central Facility provides accountability controls for STU-III Key Encryption Keying (KEK) material through the EKMS Central Facility.

c. Unkeyed STU-III terminals are unclassified, but must be afforded protection as high value Government property. However, when a terminal is keyed, it assumes the classification of the key loaded into it and must be provided physical security requirements for that level of classification.

4. Definitions. The following definitions apply:

a. Command Authority. The individual responsible for the appointment of user representative for a department, agency or organization and assigns the key ordering privileges to the User Representative. Responsible for the assignment of proper privileges, descriptors and classification to each account user. Command authority for Commander, Navy Region, Mid-Atlantic is N112.

12 JAN 2004

b. User Representative. An individual that operates as the agent of the command authority and is authorized to order keying material for that organization. User Representative for Commander, Navy Region, Mid-Atlantic is N112A.

c. User. A user is a properly cleared and authorized person who requires CMS material to accomplish an assigned duty or task. Users are responsible for the proper security, control, accountability, and disposition of material placed in their charge and must comply with the applicable security, control, and internal accountability procedures. All users will provide a signed original copy of enclosure (1) to Commander, Navy Region, Mid-Atlantic SCA prior to issuance of COMSEC material.

d. Key Storage Device (KSD). The name given to the physical device that can be used as a fill device and also as a Crypto-Ignition Key (CIK) for all STU-III's. It is a small device shaped like a physical key and contains passive memory. When it is used to carry a key to a STU-III, it is called a fill device; and when used as a protect key that has been loaded into a STU-III, it is called a CIK.

e. Crypto-Ignition Key (CIK). A KSD that contains information used to electronically lock and unlock a STU-III's secure mode. The secure mode is unlocked when the CIK is inserted and locked when it is removed.

f. Master Crypto-Ignition Key (MCIK). The first CIK created for a STU-III, which has been designated to allow the custodian to create additional CIK's whenever they are required, up to the STU-III's maximum of eight.

g. Keyed STU-III. A STU-III that has been keyed and which any of its associated CIK's is inserted.

h. Unkeyed STU-III. A STU-III that has no CIK inserted.

i. Key Encryption Key (KEK). A key used in the encryption and/or decryption of other keys for transmission or storage. There are two types of KEK's:

(1) Seed Key Encryption Key (KEK). Contains the authentication information and only permits a secure call to the EKMS Central Facility. EKMS Central Facility electronically provides an operational KEK to replace the seed KEK. Once this process, called "conversion" is complete, the STU-III may be used in the secure mode.

(2) Operational Key Encryption Key (KEK). Contains the authentication information and once loaded into a STU-III it is fully operational and secure calls can be placed.

i. Authentication Information. The information embedded as part of the key that identifies a STU-III telephone and is displayed on the distant end telephone during a secure call. The authentication information includes:

(1) The highest level of authorized classification level common to both STU-III phones.

(2) Identification of the users organization.

(3) Expiration date of the terminals key.

5. STU-III Security Requirements.

12 JAN 2004

a. Operational KEK. Operational KEK's will be afforded protection commensurate with the classification indicated on the Fill Device (FD) label.

b. Seed KEK. Seed KEK's will be afforded protection commensurate with the classification of the key to which it will be converted.

c. Master CIK's. The master CIK will be the subject of additional controls to prevent its loss or use to make unauthorized CIK's or unauthorized secure calls. Storage of the master CIK will be commensurate with the classification of the KEK with which they are associated. Master CIK's will not be issued to users for day to day usage and will be afforded the level of protection required for its classification at all times.

d. CIK's. Only authorized users will retain CIK's. Any person who is permitted unrestricted access to the keyed terminal will retain the CIK in their personal possession. If stored in the same room as the terminal, the CIK must be afforded protection commensurate with the classification of the keyed terminal (e.g., in an approved security container). The CIK could also be stored in an area apart from the terminal under the best conditions available (e.g., a locked cabinet may be sufficient).

e. Unkeyed STU-III's. Unkeyed STU-III's are unclassified. They will be provided security as a high value item.

f. Keyed STU-III's. Keyed STU-III's will be provided security at the classification level of the KEK used to load it.

6. Command Emergency Action Plan (EAP). Per reference (c), STU-III's must be incorporated into the EAP. The EAP must consider and itemize all tasks necessary to load/destroy all STU-III keying material, zeroize all loaded terminals, and account for material being destroyed which is second in importance only to the destruction itself.

a. In the event of a natural disaster during duty hours, the STU-III terminal must be disconnected from its power source.

b. If the building is being evacuated and time permits, the CIK must be removed from the terminal and locked in a classified container or kept in the personal custody of the account user.

c. If a facility is in danger of destruction and time permits, the terminal should be removed before any other high salvageable items and kept in the personal custody of the account user or turned into the custodian.

d. After the emergency has passed, the account users will report all actions taken to the custodian.

7. Zeroizing Procedures. Reference (d) provides zeroizing procedures for STU-III telephones.

8. Managing STU-III Keying Material

a. The SCA custodian is responsible for all facets of key management. All KEK requests (receipts, transfers, destructions, STU-III KEK loading, and

12 JAN 2004

creation of CIK's) must be performed by the keying material SCA custodian or alternate only.

b. STU-III operational and seed KEK's are accountable to the EKMS Central Facility by serial number from receipt by an account until destruction or transfer to another account.

c. Seed and operational KEK's are considered destroyed for accountability purposes once the terminal has been successfully keyed and a CIK has been created. Operational KEK's must be reported to EKMS Central Facility with a destruction report. Seed KEK's do not require a destruction report since they are automatically dropped after the conversion call to the central facility.

d. Increases and decreases of KEK holdings must be executed by the Keying Material SCA Custodian or alternate.

e. Local custody of keying material STU-III KEK's and master CIK's are not authorized for local custody issue to users. The custodian or alternate only must retain possession of STU-III KEK's and master CIK's at all times. Only the custodian or alternate is authorized to load key into a STU-III or create additional user CIK's with a master CIK.

f. Keying material inventories are supplied by, reported to, and reconciled with the EKMS Central Facility.

9. STU-III Maintenance Procedures. STU-III terminals that need repair must be returned to the STU-III Custodian for return to the repair facility. The terminals should be turned in to Commander, Navy Region, Mid-Atlantic N112. The custodian will require the following information:

a. Probable cause of the problem.

b. STU-III terminal with the following items:

(1) Handset with cord

(2) Power Supply with cord

10. Reportable Insecurities. The following events must be reported to the Commander, Navy Region, Mid-Atlantic EKMS Manger immediately by the user.

a. Any instance where the authentication information displayed during a secure call is not representative of the organization in which the distant terminal is located.

b. Any instance where the display indicates that the distant terminal's key has been compromised.

c. Any instance where material is left unattended, improperly stored, or material is destroyed using improper methods.

d. Any instance where there is loss of material. If the record of destruction or transfer cannot be located, then the material should be reported as lost.

e. Any instance where material is found outside of required accountability (for example, material reported as destroyed is found partially or wholly intact).

12 JAN 2004

f. Any instance where packages of material received are improperly packaged, damaged, or show evidence of tampering.

g. Any instance where individuals possessing detailed knowledge of STU-III equipment or other COMSEC material is reported in an unauthorized absence status.

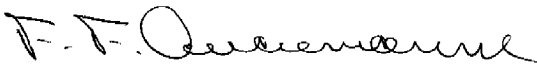
11. Insecure Practices.

a. All STU-III users must report insecure practices as soon as possible after they occur to the Commander, Navy Region, Mid-Atlantic EKMS Manager. These insecure practices are:

- (1) The loss of any CIK.
- (2) Failure to rekey a terminal within 60 days of the key's expiration date.
- (3) Transmission of classified information using a terminal whose display has failed.
- (4) Failure to protect adequately or to zeroize a CIK that is associated with a lost terminal.

b. Unless there is an indication of espionage or sabotage, insure practices are not reported outside of Commander, Navy Region, Mid-Atlantic.

c. Command action will be taken, however, to monitor and evaluate insecure practices for accessing corrective follow up action.



F. F. AUCREMANNE
Chief of Staff

DISTRIBUTION: WWW.cnrma.navy.mil

12 JAN 2004

STU-III COMSEC MATERIAL RESPONSIBILITY ACKNOWLEDGEMENT FORM

From: (Individual Person)

To: COMNAVREG MIDLANT CMS/STU-III CUSTODIAN (N112)

SUBJ: STU-III COMSEC MATERIAL RESPONSIBILITY ACKNOWLEDGEMENT

Ref: (a) COMNAVREGMIDLANTINST 2305.1A

1. I hereby acknowledge that I have read and understand reference (a).
2. I assume full responsibility for the proper handling, storage, inventorying, accounting, transfer and disposition of the STU-III COMSEC material held in my custody and/or used by me or those under my supervision.
3. I have received a copy of reference (a) from the CMS/STU-III custodian. If at any time I am in doubt as to the proper handling of the COMSEC material I am responsible for, I will immediately contact the CMS/STU-III custodian and request advice.
4. Before departing on extended leave, TAD and upon my detachment, I will check out with the CMS/STU-III custodian who will appoint a new permanent or temporary user account custodian.

SIGNATURE: _____

DATE: _____

Enclosure (1)